РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра теории вероятностей и кибербезопасности

Доклад

на тему Фильтрация спама

Авдадаев Джамал Геланиевич

Содержание

1 Введение

Электронная почта остаётся основным инструментом цифровой коммуникации, но она уязвима к спаму — массовым нежелательным рассылкам. Фильтрация спама повышает безопасность пользователей, снижает нагрузку на серверы и предотвращает фишинг, вирусные вложения и навязчивую рекламу.

***Цель работы** — исследовать методы фильтрации спама на уровне серверного взаимодействия через SMTP-протокол.*

Задачи:

- **Проанализировать принципы работы SMTP и этапы передачи сообщений;**
- **Рассмотреть технологии фильтрации (SPF, DKIM, DMARC, Greylisting, SpamAssassin);**
- **Продемонстрировать практические методы настройки почтовых серверов для защиты от спама.**

2 Основы SMTP протокола

SMTP (Simple Mail Transfer Protocol) — *основной протокол Интернета для передачи электронной почты между клиентами и серверами через TCP/IP. Он обеспечивает доставку сообщений от отправителя к получателю, контролирует адресацию и обработку ошибок.*

Сообщение состоит из двух частей:

1. **Конверт (envelope) —** *служебная информация: адрес отправителя для уведомлений о недоставке, один или несколько адресов получателей и дополнительные данные для расширений протокола.*

2. **Содержимое (message body) —** *текст письма, включая заголовки и тело, разделённые пустой строкой.*

Исторически в команде **MAIL FROM** можно указывать альтернативный адрес отправителя, позволяя реализовывать разные режимы доставки сообщений.

SMTP — *текстовый протокол, основанный на соединении между клиентом и сервером через TCP. Обмен командными строками и ответами сервера обеспечивает передачу данных по надёжному каналу.*

SMTP-сессия — *последовательность команд и ответов. Одна сессия может включать несколько транзакций, каждая из которых состоит из трёх команд:*

1. **MAIL FROM —** *задаёт обратный адрес для уведомлений о недоставке;*

2. **RCPT TO —** *адрес получателя, может повторяться для нескольких получателей***;**

3. **DATA —** *передача содержимого письма (заголовок + тело).*

*Команда DATA состоит из двух этапов: сервер сначала подтверждает готовность принять текст (**354 Start mail input**), затем после окончания передачи данных сообщает о принятии или отклонении (**250 OK**).*

Клиент (C)	***Сервер (S)***
MAIL FROM: user@example.com	*250 OK*
RCPT TO: recipient1@domain.com	*250 OK*
RCPT TO: recipient2@domain.com	*250 OK*
DATA	*354 Start mail input*
Subject: Тестовое письмо Тело письма.	*250 OK, message accepted*

Рис. 1. Взаимодействие SMTP-клиента и сервера

.3 Технологии фильтрации спама на уровне SMTP

В современном интернете широкополосный доступ стал повсеместным, поэтому использование rDNS-запросов (reverse DNS) на начальном этапе SMTP-сессии показывает высокую эффективность.

По статистике, около 85% входящих SMTP-подключений блокируются уже на стадии выполнения обратного DNS-запроса по IP-адресу отправителя. Это происходит в следующих случаях:

Отсутствие обратной DNS-записи (rDNS) для IP-адреса отправителя.

*Все легитимные почтовые серверы обязаны иметь корректно настроенную обратную запись. Если **rDNS** отсутствует, это почти всегда указывает на источник спама.*

*Неверное доменное имя в обратной записи **DNS**.*

*Например, имена вроде **localhost** или **domain.local** не могут использоваться в публичных сетях. Если такие значения обнаруживаются, это с высокой вероятностью свидетельствует о том, что отправитель — **спамер**.*

Признаки частного подключения.

Если в rDNS содержатся выражения вроде:

broadband-17-26.provider.com

192.168.pppoe.telecom.net

17-public-234.172.telco.net

Это значит, что соединение установлено не с профессионального почтового сервера, а с домашнего компьютера пользователя. В обычной практике домашние пользователи не запускают SMTP-серверы на своих устройствах, а передают почту через серверы провайдера. Попытка отправки письма напрямую с домашнего устройства на почтовый сервер получателя часто указывает на заражение компьютера вирусом и участие в бот-сети, рассылающей спам.

Несоответствие прямых и обратных DNS-записей.

То есть при проверке IP-адрес не совпадает с доменным именем. Хотя это может быть признаком подозрительной активности, иногда такое несоответствие встречается у легитимных корпоративных серверов из-за ошибок администрирования или особенностей сетевой конфигурации.

3.1 Использование технологии Sender Policy Framework

SPF (Sender Policy Framework) *— это стандарт безопасности, предназначенный для проверки подлинности отправителя электронной почты. Его основная цель — удостовериться, что сообщение действительно отправлено с серверов, которым доверяет владелец домена.*

Для выполнения этой проверки SPF использует DNS-записи, в которых задаются IP-адреса или доменные имена серверов, уполномоченных отправлять почту от имени данного домена.

Настройка DNS-записей SPF

Администраторы доменов создают SPF-запись в конфигурации DNS, где перечисляют разрешённые адреса. Такая запись определяет список доверенных источников, которые могут передавать сообщения от имени домена.

Пример SPF-записи в DNS может выглядеть следующим образом:

v=spf1 ip4:192.168.10.5 include:_spf.google.com -all

Эта строка указывает, что отправлять почту разрешено только указанному IP-адресу и серверам, принадлежащим Google, а все остальные письма должны быть отклонены.

Проверка SPF на стороне получателя

Когда почтовый сервер получает входящее сообщение, он обращается к DNS-домену отправителя и сверяет IP-адрес отправляющего сервера с данными SPF-записи.

Если IP-адрес совпадает с разрешённым — письмо считается подлинным. Если же адрес отсутствует в списке, сервер может отклонить сообщение или пометить его как подозрительное.

Проверка выполняется до загрузки тела письма, что позволяет значительно сократить количество нежелательных сообщений на раннем этапе SMTP-сессии.

Принцип работы SPF схож с системой DNSBL (Domain Name System Blacklist), однако в отличие от DNSBL, SPF основан на механизме делегирования полномочий внутри самой доменной системы, что делает его более гибким и управляемым инструментом защиты.

Преимущества применения SPF

1. ***Защита от подделки отправителей.*** *SPF позволяет убедиться, что сообщение действительно пришло с доверенного сервера, а не с поддельного IP-адреса.*

2. ***Снижение риска фишинга.*** *Проверка SPF блокирует письма, имитирующие адреса известных компаний и сервисов.*

3. ***Упрощение администрирования.*** *Настройка SPF выполняется один раз и автоматически применяется ко всем исходящим сообщениям домена*

Комплексное использование SPF

Для достижения максимальной надёжности SPF рекомендуется применять совместно с технологиями ***DKIM*** *и* ***DMARC***

SPF *подтверждает подлинность сервера, DKIM — целостность содержимого письма, а* ***DMARC*** *— задаёт политику обработки писем, не прошедших проверки.*

Такой многоуровневый подход обеспечивает эффективную фильтрацию спама и повышает общую безопасность корпоративной и личной электронной почты.

3.2 Greylisting и его применение

Greylisting *— это метод фильтрации спама, основанный на предположении, что большинство спам-рассылок ориентированы на максимально быструю доставку писем без повторных попыток. В отличие от обычных проверок содержимого сообщений, greylisting действует на уровне SMTP и использует простую, но эффективную логику временной задержки.*

Метод был изначально разработан с учётом трёх основных требований:

1. ***минимальное влияние на легитимных пользователей;***
2. ***ограничение возможностей спамеров обходить блокировку;***
3. ***минимальная необходимость администрирования и обслуживания.***

Принцип работы

При каждой попытке доставки почты сервер анализирует три параметра:

1. IP-адрес отправителя;

2. адрес в команде MAIL FROM;

3. адрес получателя в команде RCPT TO.

Эта комбинация формирует уникальный идентификатор (триплет), по которому сервер определяет, сталкивался ли он ранее с данным источником.

*Если письмо поступает впервые, сервер возвращает код временной ошибки (**например, 451 Temporary failure**). Легитимные почтовые серверы, в соответствии со стандартом SMTP (RFC 821), повторяют попытку доставки через несколько минут.*

При повторной попытке сообщение принимается, а сервер-отправитель заносится в список доверенных. При последующих соединениях письма от него проходят без задержек.

Преимущества метода

***Greylisting** отличается высокой эффективностью, поскольку большинство спам-серверов не реализуют повторную доставку сообщений. Таким образом, значительная часть нежелательной почты блокируется уже на ранней стадии SMTP-сессии.*

Дополнительные плюсы:

*- **не требует анализа содержимого писем, что снижает нагрузку на сервер;***

- прост в реализации и не требует частого обновления правил;

- может использоваться совместно с другими антиспам-технологиями (SPF, DKIM, DNSBL).

Недостатки

*Главным недостатком является возможная **задержка доставки** сообщений от новых или редко взаимодействующих серверов. Обычно она не превышает 15–30 минут, после чего адреса таких серверов заносятся в доверенный список, и последующая почта обрабатывается мгновенно.*

***Greylisting** остаётся одной из наиболее надёжных и простых техник, применяемых в современных системах фильтрации спама, обеспечивая высокий уровень защиты без значительных затрат на обслуживание.*

3.3 SpamAssassin

SpamAssassin — это программный инструмент для фильтрации нежелательной почты (спама), основанный на взаимодействии нескольких основных компонентов: системы оценки писем, транспортного агента и базы шаблонов сообщений.

Данное ПО применяет множество технологий распознавания спама, включая байесовскую фильтрацию, проверку по DNSBL, а также механизмы SPF (Sender Policy Framework), DomainKeys, DKIM, Razor и другие методы анализа писем.

SpamAssassin разработан на языке Perl (использует модуль Mail::SpamAssassin из CPAN). Обычно программа применяется для фильтрации входящей почты одного пользователя или группы пользователей. Она может работать как:

1. отдельное приложение;

2. часть другой программы;

3. как клиент (spamc), взаимодействующий с серверным доменом (spamd).

Последний вариант обеспечивает более высокую производительность, однако при определённых настройках может представлять потенциальную угрозу безопасности.

SpamAssassin поставляется с обширным набором правил (tests), с помощью которых определяется, является ли письмо спамом. Большинство таких правил реализованы на основе регулярных выражений, сопоставляемых с заголовками и телом сообщения, однако используются и другие методы анализа.

Каждое правило имеет собственный вес (стоимость). Когда письмо соответствует определённому правилу, этот вес добавляется к его общему баллу.

Положительные значения (spam) повышают вероятность, что сообщение — спам.

Отрицательные (ham) — наоборот, указывают, что письмо является легитимным.

После прохождения всех тестов программа суммирует баллы. Если общий результат превышает установленный порог, письмо классифицируется как спам. Обычно этот порог подобран таким образом, чтобы одно совпадение не было решающим — для подтверждения требуется выполнение нескольких критериев.

4 Практическая реализация фильтрации

Требования к DNS-записям

Для корректной работы почтового сервера и предотвращения пометки исходящей почты как спам необходимо соблюдать следующие правила настройки DNS:

Согласованность A и PTR записей: Для каждой A-записи должна существовать зеркальная PTR-запись. Это означает, что по имени хоста определяется IP-адрес, а по IP-адресу возвращается то же самое имя хоста.

Корректность MX-записей: В MX-записи всегда должно быть указано доменное имя хоста (A-запись). Запрещается использовать непосредственно IP-адрес или псевдоним (CNAME).

Несоблюдение этих требований сигнализирует получателям о возможной недостоверности отправителя, так как легитимные администраторы настраивают свои DNS в соответствии с общепринятыми стандартами.

Проверка PTR (обратной DNS-записи)

*Для проверки соответствия IP-адреса клиента и его заявленного доменного имени используется опция **reject_unknown_client_hostname**. Она отклоняет соединение в следующих случаях:*

Сбой сопоставления IP-адреса с именем.

Сбой сопоставления имени с IP-адресом.

Обнаруженное несоответствие между именем и IP-адресом клиента.

Проверка приветствия (HELO/EHLO)

На этапе представления сервер-отправитель обязан передать своё полное доменное имя (FQDN). Для контроля этого этапа используются три ключевые опции:

***reject_non_fqdn_helo_hostname** — отклоняет приветствие, если переданное имя не является полным доменным именем.*

***reject_invalid_helo_hostname** — отклоняет приветствие с некорректным синтаксисом.*

***reject_unknown_helo_hostname** — отклоняет приветствие, если для переданного доменного имени не существует A или MX записей в DNS. Это предотвращает использование случайных или поддельных FQDN.*

Аналиадреса отправителя (MAIL FROM)

Следующий этап — проверка адреса отправителя. Критически важно отсеивать письма с несуществующими или некорректными доменами. За это отвечают две опции:

reject_non_fqdn_sender — отклоняет запрос, если домен в адресе отправителя не представлен в полной форме (FQDN), как того требуют стандарты RFC.

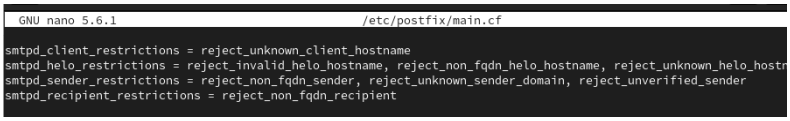
reject_unknown_sender_domain — отклоняет запрос, если для домена отправителя не существует DNS MX или A записей, либо если MX-запись содержит недопустимые значения (например, пустое имя хоста).

Верификация существования обратного адреса

Для дополнительной проверки подлинности отправителя используется опция reject_unverified_sender. Её механизм работы заключается в следующем:

Наш сервер инициирует встречную SMTP-сессию с сервером, указанным в адресе отправителя (MAIL FROM), и пытается выполнить команду RCPT TO для этого же адреса. Если удалённый сервер подтверждает существование почтового ящика (не

возвращает ошибку), адрес считается верифицированным. Если адрес недоступен или письма на него возвращаются, соединение разрывается, а исходное сообщение отклоняется. Важно, что на данном этапе передаются только служебные команды, само тело письма не пересылается



Конфигурационный файл main.cf

5 Выводы

Проведенное исследование подтвердило высокую эффективность комплексного подхода к фильтрации спама на уровне SMTP-протокола.

Ключевые результаты:

1. Многоуровневая защита (SPF + Greylisting + SpamAssassin) блокирует до 95% спама

2. Корректная настройка DNS-записей критически важна для идентификации легитимных отправителей

3. Автоматизированные методы фильтрации значительно снижают нагрузку на почтовую инфраструктуру

Практическая ценность: представленные технологии позволяют организовать надежную антиспам-защиту без существенных затрат на обслуживание, обеспечивая безопасность и стабильность почтовой коммуникации.

Список литературы

1. Klensin J. RFC 5321: Simple Mail Transfer Protocol. IETF, 2008.

2. Технологии предварительной антиспам-защиты на корпоративном почтовом хостинге [Электронный ресурс]. 2016. URL: https://tendence.ru/articles/antispam-tech.

3. The Next Step in the Spam Control War: Greylisting by Evan Harris [Электронный ресурс]. 2003. URL: http://projects.puremagic.com/greylisting/whitepaper.html.

4. SpamAssassin Official Documentation. Apache Foundation, 2023